Janice K. Brewer
Governor

Scott A. Smith
Director

ARIZONA DEPARTMENT OF ADMINISTRATION

OFFICE OF THE DIRECTOR

100 NORTH FIFTEENTH AVENUE • SUITE 401
PHOENIX, ARIZONA 85007

(602) 542-1500

August 20, 2012

Debra K. Davenport, CPA
Auditor General
Office of the Auditor General
2910 North 44th Street, Suite 410
Phoenix, Arizona 85018

Re: Auditor General Audit of ADOA State Data Center, Draft Report dated July 24, 2012

Dear Ms. Davenport:

Thank you for the opportunity to review and comment on the Auditor General ADOA State Data Center Audit. We appreciate the professionalism and efforts of the audit team and believe that the implementation of the findings will further enhance the efficiency and effectiveness of our Agency.

Enclosed are our responses to each recommendation in the report, in the order they are listed. Our responses to your findings are generic due to the sensitivity of the security findings.

Thank you again for the opportunity to respond. Should you have any questions or would like additional information, please do not hesitate to contact me at (602) 542-1500.

Sincerely,

Scott A. Smith
Director

Enclosures

ADOA Agency Response, by Section and Finding

Auditor General Recommendations – ADOA State Data Center

Recommendation 1.1

A. The Department should:
   a. Create and formalize a comprehensive disaster recovery plan, which includes all system and infrastructure components for which it is responsible, and addresses important elements such as regulatory and contractual requirements, the Departments overall business continuity needs, IT resource management requirements and interdependencies, an analysis of business impacts, risk assessments, emergency procedures, testing and ongoing maintenance of its disaster recovery efforts.
   b. Formally document and publish the plan. The plan should include information related to the activation and notification, recovery and reconstitution phases and should include supporting documentation.
   c. Test the plan on a regular basis using realistic scenarios, as defined in the plan documented and make modifications when necessary to correct any problems identified through testing.

B. The Data Center should establish formal procedures and benchmarks to ensure that customers who contract with it for disaster recovery services receive the services in accordance with agreed-upon benchmarks and service guarantees. The procedures should ensure that customers' systems are appropriately identified, listed, prioritized and handled in accordance with relative importance.

C. The Data Center should better publicize to its open systems customers the services it provides to them and clarify the roles and responsibilities that its customers play in disaster recovery efforts. This information should be included in contracts for services and provided in summary form to the appropriately responsible individual at the customer organization.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 1.2

The Data Center should establish, implement and maintain a formal inventory and a documented process for identifying and categorizing its organization-critical and high-risk assets. The IT inventory should contain information on applications, data, hardware, software, network resources and services, and facilities; and should assign corresponding security risk ratings to these assets.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 1.3

To help ensure that sensitive data is properly protected, the Department should:

A. Complete its development, review and implementation of a documented organization-wide data classification policy and process.

B. Ensure that its process is based on risks and requirements such as confidentiality and sensitivity of the information, consisting of an inventory of information classification details that include assigned classification, identity of the information owner, and a brief description of information classified; and that it is communicated to all affected parties, reviewed and updated regularly.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 2.1

The Department should establish and implement a process for performing risk assessments that assigns responsibility, mandates regular assessments, contains a structured methodology for assessing risks, documents results and potential impact of results, uses results to make changes to the organization's security program, and reports results to top management. Additionally, the Department should perform risk assessments on an annual schedule or as significant changes are made to information resources as outlined in its current policy.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 2.2

The Department should establish and implement a formal security compliance process, which consists of obtaining regular confirmation of compliance from process owners, ensuring that internal and external compliance reviews are performed against internal policies, and implementing a process to monitor and report on non-compliance issues. As a component of its compliance process, the Department should include an enforcement mechanism to ensure that policies are effective and are being followed.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 2.3

A. The Department should enhance its policy related to security awareness training to include adequate guidance on what should be included in such training-and training materials-being sure to address all areas required by state policy; and should develop mechanisms to ensure that the policy is being followed by all of it Business Units.

B. As required by state policy, the Department should establish a department-wide security awareness education and training program. The program should:
   a. Be designed to ensure that employees understand relevant IT security risks and threats, the Department's IT-related security policies and each individual's role in carrying out those policies.
   b. Incorporate a mechanism to periodically evaluate the programs effectiveness and make changes to it as necessary.
   c. Consider and address the type and form of training needed relevant to staff member's roles and functions.
   d. Be provided annually, or upon occurrence of a specific event, such as a change in job responsibilities or employment status.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 2.4

The Department should:

A. Ensure that security policies are followed and security mechanisms are in use for all applications and systems.

B. Review the configuration of its servers to ensure that only needed services are running, that services and associated users and system accounts are configured securely, and that critical services are segmented from those available through the public network.

C. Use its network vulnerability scanning software or perform other procedures to regularly treat all segments of its network, identify potential vulnerabilities, and mitigate them to the extent possible.

D. Develop and implement a configuration management policy that covers its IT resources and addresses security considerations.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 2.5

The Department should complete, approve and implement an organization-wide policy and process for incident response management. It should ensure that all the appropriate Business Units are involved and that the policies and procedures identify roles and responsibilities over incident handling, provide responding individuals with a clear incident handling, provide responding individuals with a clear plan and authority to make critical decisions, and provide information on how to identify, respond to, recover from, and follow up on incidents.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 2.6

A. The Data Center should develop and implement log management policies and procedures. Those procedures should ensure that all important system, application and security-related events be defined and recorded in logs, stored centrally, protected against unauthorized change, and analyzed on a regular basis.

B. The Department should establish and implement formalized procedures to ensure that audit logs are regularly reviewed for critical events and that any

unauthorized activity detected is investigated and addressed in a timely manner.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 3.1

A. The Department should ensure that all of its Business Units are adhering to the Data Center's Access Control Policy, which provides guidance on: a) ensuring all user accounts are uniquely identifiable and assigned to an individual employee; and b) periodically reviewing all user access lists to ensure that they are still needed, establish user identification, and enforce access rights appropriate to the person's job duties and responsibilities.

B. The Department should review the use of generic user accounts and should eliminate ones that are no longer needed and implement procedures to better monitor ones that are retained.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 3.2

A. The Department should ensure that all of its Business Units are adhering to the Access Control Policy by removing user accounts when an employee is no longer employed, and regularly reviewing access lists to identify changes needing such action.

B. Determine what problems exist with the system used to inactivate network employee accounts based on pay status and correct them, or develop alternate procedures to ensure that proper action is taken.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 3.3

A. The Department should take steps to ensure that it maintains required authorization documentation on file for all new account creation requests as outlined in its policy.

B. Management should regularly conduct a review of a sample of user accounts to ensure compliance with its policy.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 4.1

The Data Center should:

A. Complete development of change management policies and procedures, to include:
   a. Roles and responsibilities;
   b. Classification and prioritization of all changes based on business risk;
   c. Assessment of impact;
   d. Authorization and approval of all changes by the business process owners and IT;
   e. Testing plans;
   f. Tracking and status of changes;
   g. Impact of data integrity;
   h. Emergency changes;
   i. Tracking, status and reporting of changes; and
   j. Change closure.

B. Require the Change Control Form to be completed consistently and maintained for all changes, and to be updated to include all necessary items, such as impact analysis and testing plans.

C. Consistently maintain all relevant documentation for each change in a central repository or location.

D. Review the change control process in use by the Enterprise Infrastructure and Communications (EIC) Office and consider its applicability to the Data Center's broader IT requirements. If deemed appropriate, consider incorporation of relevant EIC practices into the Data Center's existing process.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will

be implemented.

Recommendation 4.2

The Data Center should develop and implement a documented, organization-wide configuration management process that is in line with IT standard best practice and state requirements. The process should include defined responsibilities, consistent identification of configurations of IT devices, network components, documented change control, tracking of configuration items, and periodic review of configurations.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented.

Recommendation 5.1

The Department should

A. Perform a comprehensive review of its IT policies and procedures, comparing them against state-wide standards and IT best practices to 1) identify missing items, and 2) items that are incomplete, out of date, or not in use.

B. Prioritize the results from its review and develop and implement, where necessary, effective IT policies and procedures that align with business requirements and then monitor for compliance with its policies and procedures.

C. Develop a strategy that ensures that IT policies and procedures are effectively and consistently communicated and disseminated to all affected parties within the Department.

Agency Response:

The finding of the Auditor General is agreed to and the audit recommendation will be implemented